

**UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION**

IN THE MATTER OF THE SEARCH OF)	CASE NO.:
799 LAVINIA ROAD)	
WINNSBORO, SOUTH CAROLINA)	(Under Seal)
)	
)	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Special Agent Christian L. Cavaliere, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of residence described in Attachment A of this Affidavit. I am a Special Agent with the Drug Enforcement Administration (DEA), United States Department of Justice, and I have served in that capacity since March 2019. I am currently assigned to the Provisional Task Force Group with the Columbia Division of the DEA in Columbia, South Carolina. As a Special Agent of the DEA, I am authorized to conduct investigations and make arrests for violations of Title 18 and Title 21 of the United States Code. I have participated as a Co-Case Agent and Investigative Agent in multiple narcotics investigations which have utilized many enhanced investigative techniques such as Title III wire intercepts, search warrants, and forensic examinations of varying electronic devices. I have been the Affiant for numerous search warrant applications. As an Investigative Agent, I have received advanced specialty training in areas including the interception of telephone communications, fundamentals of telecommunications, electronic forensics, data analysis, cellular analysis, as well as having received extensive training in advanced Narcotics investigations.

2. Through my training, education, and experience, I have become familiar generally with the manner in which illegal drugs are imported and distributed, the method of payment for such drugs, and the efforts of persons involved in such activity to avoid detection by law enforcement. Additionally, I have received training, both formal and informal, in the

operation of drug trafficking, money laundering, and wiretap investigations.

3. Based upon my training and experience, as well as the other sources of information indicated above, I know the following:

- a) Drug traffickers frequently store controlled substances and drug paraphernalia for packaging, diluting, weighing and/or distributing controlled substances in, on, and around residence and/or business, and within vehicles and/or structures located on their property or its surrounding curtilage in an effort to avoid detection by law enforcement. This paraphernalia often includes but is not limited to: scales, plastic bags, diluting agents, etc;
- b) Drug traffickers frequently store currency, financial instruments, precious metals, jewelry, and other items of value, which are the proceeds of drug transactions inside, on, and around their residence and/or place of business;
- c) Drug traffickers frequently have in their possession, whether on their person, inside their vehicle, or in, on, or around their residence, firearms and other weapons. These firearms and weapons are commonly used by drug traffickers to protect their property, including, but not limited to: controlled substances; drug proceeds in the form of currency, jewelry and other real property; and other items of value whose existence may be considered illegal;
- d) Drug traffickers frequently maintain in their residence and/or business, records of drug transactions, including notes, ledgers, receipts, computer files, photographs, video tapes, digital video recorders and associated hard drives memorializing footage generated by closed circuit or internet-based video camera systems, telephone records, calling cards, and correspondence which contain information on current and past associates, and may be used to identify co-conspirators who have not been identified or located;

- e) Drug traffickers frequently maintain fictitious identification and other documents which are intended to conceal their identity and avoid detection by law enforcement, including fictitious driver licenses, passports, photo identification cards, and documents relating to fraudulently obtained vehicle titles, registrations, and insurance;
 - f) Drug traffickers frequently maintain in their residence currently and previously used wireless telephones and/or electronic communications devices. Drug traffickers frequently store digital and voice messages and phone numbers, belonging to drug purchasers, other drug traffickers, and various individuals or entities working or assisting in the drug trade;
 - g) Drug traffickers regularly use computers in furtherance of drug trafficking and money laundering crimes, by maintaining illegal records and ledgers on the hard drives (or associated removable media) of said computers. Drug traffickers and money launders also regularly use computers to communicate with one another by way of e-mail, or other telecommunications devices using voice over internet protocol (VOIP), which work in conjunction with computers;
 - h) Drug traffickers and money launderers maintain books, records, receipts, notes, ledgers, currency and papers which are evidence of the commission of their narcotics and money laundering offenses. The records include tally or ledger sheets; sales and/or purchase invoices; bank, wire transfer and/or other financial institution records; federal and state corporate, partnership, individual and/or other tax and informational returns filed or required to be filed;
4. Drug traffickers frequently engage in money laundering in an effort to conceal the proceeds derived from the distribution of illegal drugs and present them as legitimate revenues. Drug traffickers and money launderers will also regularly utilize drug proceeds to procure goods (including but not limited to real estate, jewelry, automobiles, electronics, etc.) and services which will be used in the course of a legitimate business venture. Drug traffickers often

use drug proceeds to acquire and/or operate ostensibly legitimate businesses to provide a front for their illegal activity and to facilitate the laundering of drug proceeds;

- a) Drug traffickers and money launderers will regularly purchase goods and services using alias names, nominee names, or the names of criminal associates engaged in the ongoing drug trafficking or money laundering enterprise, or under the name(s) of a business or organization ultimately controlled and/or operated by the drug trafficking or money laundering organization; and
- b) Drug traffickers frequently store currency in multiple locations to avoid discovery and seizure of all drug proceeds from law enforcement during an arrest and/or search.

PREMISES TO BE SEARCHED AND ITEMS TO BE SEIZED

- 5. This affidavit is being submitted in support of an application for a search warrant for a residence located at 799 Lavinia Road, Winnsboro, South Carolina (**TARGET LOCATION**) (described further in Attachment A).
- 6. Also to be searched are all sheds, outbuildings, appurtenances, and vehicles associated with the **TARGET LOCATION** as well as the electronic contents of any computers, removable media (including thumb drives, removable hard drives, compact discs, or any other device which can maintain digital/electronic data), digital video recorders or hard drives, wireless telephones, or other telecommunications devices located at the premises, or within any sheds, outbuildings, appurtenances, and vehicles associated with the property.
- 7. The items to be seized at the **TARGET LOCATION** are described more fully in Attachment B.

PROBABLE CAUSE

8. On June 16, 2021, agents with the FBI, DEA and numerous local partner agencies conducted coordinated arrests of numerous individuals indicated in a federal drug trafficking conspiracy case.
9. One of the indicted individuals, Antonio Goins, was located and arrested at **TARGET LOCATION**.
10. Agents announced their presence and Goins refused to come to the door of the residence for approximately twenty minutes residence. Agents could hear rustling inside and observed Goins' vehicle outside the location. Agents observed Goins white 2010 Chevrolet Silverado bearing South Carolina license plate TIN924, registered to GOINS, with a "Tony's Garage Door," and telephone number 803-667-2946 on the rear window of the truck. Based on intelligence gathered during the investigation, agents are aware telephone number 803-667-2946 is associated with Goins based on a Richland County Sheriff's Department November 19, 2020, incident report, where Goins reported himself as a victim of a stolen tractor. Agents entered the entryway of the residence and began searching for occupants. Agents were able to locate Goins inside the residence. Upon observing Goins person, agents observed material covering Goins t-shirt consistent with attic insulation. Agents then began doing a protective sweep for other occupants. During the protective sweep, agents observed a vent, large enough to fit a person, had been disturbed. Upon searching the vent for a person, agents noticed a firearm consistent with the size and shape of a rifle. Goins is prohibited from possessing a firearm from a prior conviction. Goins further informed agents, post-*Miranda*, that he also had marijuana in his refrigerator, and was knew that he was unable to possess a firearm due to his criminal history. No other occupants were located in the residence other than Goins.

Furthermore, I believe evidence of these violations are located at the **TARGET LOCATION**.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS OF COMPUTERS
AND CELLULAR TELEPHONES**

11. I know through my training and experience that drug dealers frequently communicate with their customers and suppliers using cellular telephones.
12. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.
13. There is reasonable cause to believe that phones and/or other electronic devices or storage media may be maintained in and among records kept on the premises. As described above and in Attachment B, this application seeks to search for such records in whatever form they are found. Thus, the warrant applied for would authorize the seizure of cellular telephones, computers and other electronic storage media, or potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). I submit that if a computer, cell phone or storage media is found, on the premises, there is probable cause to believe records will be stored on that computer, or storage medium for at least the following reasons:
- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
 - c) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
14. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on devices in the **TARGET LOCATION** because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

15. *Necessity of seizing entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for and who has used it requires considerable time and taking that much time on premises can be unreasonable.
- b) Technical Requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software and configurations. Therefore, search them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system or its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

17. Based on the above facts and circumstances, your Affiant believes there is probable cause to believe that evidence of violations of federal drug trafficking statutes will be found at the **TARGET LOCATION**. I am aware through training and experience large scale drug traffickers will often have a drug source of supply out of state which often precludes meeting their source of supply in person. Therefore, traffickers will utilize various electronic devices to contact and coordinate the payment and delivery of controlled substances to them. Payments to out of state drug sources of supply frequently require utilizing bank deposits, purchasing money orders, shipping bulk cash, or electronic payments through services such as Cash App. All of these methods generate physical or electronic records which are highly evidentiary for a drug trafficking investigation. Additionally, drug traffickers will often maintain a ledger of payments and debts with individuals with whom they are involved in the sale of controlled substances. These ledgers regularly document the amount of drugs sold, dates which controlled substances were sold, payments/debt for these sales and identifying information who purchased the controlled substances.
18. Due to the information contained in this affidavit, I believe there is reason to believe evidence of drug trafficking will be located within the **TARGET LOCATION** in physical and electronic form. Therefore, your Affiant requests that a search warrant be issued for the property described herein, and more particularly described in Attachment A to search for the items enumerated in Attachment B. This Affiant knows these items to be tangible evidence of violations of Title 21, U.S.C. Sections 841(a)(1) (possession with intent to


distribute a controlled substance), 843(b) (use of a communication device for drug trafficking), and 846 (conspiracy to distribute a controlled substance).



CHRISTIAN L. CAVALIERE
SPECIAL AGENT
DRUG ENFORCEMENT AGENCY

SWORN TO ME VIA TELEPHONE OR
OTHER RELIABLE ELECTRONIC MEANS
AND SIGNED BY ME PURSUANT TO
FED. R. CRIM. P. 4.1 AND 4(d) OR 41(d)(3),
AS APPLICABLE

This 16th day of June 2021
Greenville, South Carolina



SHIVA V. HODGES
UNITED STATES MAGISTRATE JUDGE